

When it all comes down to dust
 I will kill you if I must,
 I will help you if I can.
 And mercy on our uniform,
 man of peace or man of war,
 the peacock spreads his fan.

To Yuri Bilu, colleague and
 friend for all seasons.¹

ON THE EQUATION $X^n - 1 = BZ^n$

B. BARTOLOMÉ AND P. MIHĂILESCU

ABSTRACT. We consider the Diophantine equation $X^n - 1 = BZ^n$, where $B \in \mathbb{Z}$ is understood as a parameter. We prove that if the equation has a solution, then either the Euler totient of the radical, $\varphi(\text{rad}(B))$, has a common divisor with the exponent n , or the exponent is a prime and the solution stems from a solution to the diagonal case of the Nagell–Ljunggren equation: $\frac{X^n-1}{X-1} = n^e Y^n$, $e \in \{0, 1\}$. This allows us to apply recent results on this equation to the binary Thue equation in question. In particular, we can then display parametrized families for which the Thue equation has no solution. The first such family was proved by Bennett in his seminal paper on binary Thue equations [Be].

Binary Thue Equation, Nagell-Ljunggren Equation

1. INTRODUCTION

Let $B, n \in \mathbb{N}_{>1}$ be such that

$$(1) \quad \varphi^*(B) := \varphi(\text{rad}(B)) \quad \text{and} \quad (n, \varphi^*(B)) = 1.$$

Here $\text{rad}(B)$ is the radical of B and the condition implies that B has no prime factors $t \equiv 1 \pmod{n}$. In particular, none of its prime factors splits completely in the n -th cyclotomic field.

More generally, for a fixed $B \in \mathbb{N}_{>1}$ we let

$$(2) \quad \mathcal{N}(B) = \{n \in \mathbb{N}_{>1} \mid \exists k > 0 \text{ such that } n \mid \varphi^*(B)^k\}.$$

If p is an odd prime, we shall denote by CF the combined condition requiring that

- I The Vandiver Conjecture holds for p , so the class number h_p^+ of the maximal real subfield of the cyclotomic field $\mathbb{Q}[\zeta_p]$ is not divisible by p .
- II The index of irregularity of p is small, namely $i_r(p) < \sqrt{p} - 1$, so there are $i_r(p)$ odd integers $k < p$ such that the Bernoulli number $B_k \equiv 0 \pmod{p}$.

¹ "Story of Isaac", by Leonard Cohen.

Date: Version 1.13 July 1, 2015.

The second condition was discovered by Eichler, as a sufficient condition for FLT1 to be true. It is known from recent computations of Buhler and Harvey [BH] that the condition CF is satisfied by primes up to $163 \cdot 10^6$.

We consider the binary Thue equation

$$(3) \quad X^n - 1 = B \cdot Z^n,$$

where solutions with $Z \in \{-1, 0, 1\}$ are considered to be trivial. The assertion that equation (3) has finitely many solutions other than the trivial ones is a special case of the general Pillai conjecture (Conjecture 13.17 of [BBM]). This equation is encountered as a particular case of binary Thue equations of the type

$$(4) \quad aX^n - bY^n = c,$$

see [BGMP]. In a seminal paper [Be], Michael Bennett proves that in the case of $c = \pm 1$ there is at most one solution for fixed $(a, b; n)$ and deduces that the parametric family $(a + 1, a; n)$ has the only solution $(1, 1)$ for all n . The equation (3) inserts naturally in the family of equations (4), with $a = c = \pm 1$.

A conjecture related directly to (3) states that

Conjecture 1.1. *Under (1), Equation (3) has no other non-trivial solution than $(X, Y; B, n) = (18, 7; 17, 3)$.*

Current results on (3) are restricted to values of B which are built up from small primes $p \leq 13$ [G]. If expecting that the equation has no solutions, – possibly with the exception of some isolated examples – it is natural to consider the case when the exponent n is a prime. Of course, the existence of solutions (X, Z) for composite n imply the existence of some solutions with n prime, by raising X, Z to a power.

The main contribution of this paper will be to relate (3) in the case when n is a prime and (1) holds, to the diagonal Nagell – Ljunggren equation,

$$(5) \quad \frac{X^n - 1}{X - 1} = n^e Y^n, \quad e = \begin{cases} 0 & \text{if } X \not\equiv 1 \pmod{n}, \\ 1 & \text{otherwise.} \end{cases}$$

This way, we can apply results from [Mi2] and prove the following:

Theorem 1.2. *Let n be a prime and $B > 1$ an integer with $(\varphi^*(B), n) = 1$. Suppose that the equation (3) has a non trivial integer solution different from $n = 3$ and $(X, Z; B) = (18, 7; 17)$. Let $X \equiv u \pmod{n}$, $0 \leq u < n$ and $e = 1$ if $u = 1$ and $e = 0$ otherwise. Then:*

A $n > 163 \cdot 10^6$.

B $X - 1 = \pm B/n^e$ and $B < n^n$.

C If $u \notin \{-1, 0, 1\}$, then condition CF (II) fails for n and

$$\begin{aligned} 2^{n-1} &\equiv 3^{n-1} \equiv 1 \pmod{n^2}, & \text{and} \\ r^{n-1} &\equiv 1 \pmod{n^2} & \text{for all } r | X(X^2 - 1). \end{aligned}$$

If $u \in \{-1, 0, 1\}$, then Condition CF (I) fails for n .

The particular solution $n = 3$ and $(X, Z; B) = (18, 7; 17)$ is reminiscent of a solution of the diagonal Nagell solution; it is commonly accepted that the existence of non trivial solutions tends to render Diophantine equations more difficult to solve. Based on Theorem 1.2 we prove nevertheless the following

Theorem 1.3. *If equation (3) has a solution for a fixed B verifying the conditions (1), then either $n \in N(B)$ or there is a prime p coprime to $\varphi^*(B)$ and a $m \in N(B)$ such that $n = p \cdot m$. Moreover X^m, Y^m are a solution of (3) for the prime exponent p and thus verify the conditions in Theorem 1.2.*

This is a strong improvement of the currently known results.

Remark 1.4. *Theorem 1.2 uses criteria from the diagonal case of the Nagell-Ljunggren equation, the relation being established by point (B) of the theorem. The criteria were proved in [Mi2] and are in part reminiscent from classical cyclotomic results on Fermat's Last Theorem. Thus, the criteria for the First Case, which are enounced in point (C) are the Eichler criterion CF (II) and the criteria of Wieferich and Furtwängler (cf. Theorem 2 in [Mi2]). For the Second Case of Diagonal Nagell-Ljunggren, in point (C), it was possible to restrict the two conditions proved by Kummer for the FLTII to the single condition CF (I), namely Vandiver's conjecture (cf. Theorem 4 in [Mi2]). This is a consequence of the fact that unlike FLT, Nagell-Ljunggren is a binary equation, a fact which allowed also to prove upper bounds for the solutions, which are given in Theorem 2.2 below. The fact that the Nagell-Ljunggren equation is not homogenous in X makes it difficult to prove lower bounds, thus leaving a gap on the way to a complete proof of Conjecture 1.1.*

The proofs in [Mi2] used methods that generalize the ones that helped proving the Catalan Conjecture [Mi1]. A variant of these methods will be applied for proving point (B). We gathered the occasion of writing this paper to give in the Appendix an extensive exposition of the computations on which the singular case in the proof the respective estimate from [Mi2] relies: some colleagues had pointed out that they could not verify the computation on base of the arguments in [Mi2], so this difficulty should be dealt with in the Appendix.

The plan of the paper is as follows: in Section 2 we establish the connection between equations (3) and (1.2), review some basic properties of Stickelberger ideals and prove auxiliary technical lemmata concerning coefficients of binomial series development.

With these prerequisites, we complete the proof of Theorem 1.2 in Section 3. Given the reduction to the Nagell-Ljunggren Diagonal Case, the proof focuses on point (B) of Theorem 1.2. In Section 4 we drop the condition that n be a prime and use the proven facts in order to deduce the results on (3) for arbitrary exponents n which are stated in Theorem 1.3. Finally, the Appendix provides the details for an estimate used in [Mi2], as mentioned in Remark 1.4.

2. PRELIMINARY RESULTS

The proof of Theorem 1.2 emerges by relating the equation (3) to the Diagonal Case of the Nagell – Ljunggren conjecture. In this section we shall recall this conjecture and several technical tools used for reducing one conjecture to the other. The reduction is performed in the next section.

2.1. Link of (3) with the diagonal Nagell – Ljunggren equation. We note that $\delta = \left(\frac{X^n-1}{X-1}, X-1\right)$ divides n and $\delta = n$ exactly when $X \equiv 1 \pmod{n}$. Indeed, from the expansion

$$\frac{X^n - 1}{X - 1} = \frac{((X - 1) + 1)^n - 1}{X - 1} = n + k(X - 1),$$

with $k \in \mathbb{Z}$, one deduces the claim $\delta | n$. If $u \neq 1$, then $\delta = n$ and thus $n | (X - 1)$ must hold. Conversely, inserting $X \equiv 1 \pmod n$ in the previous expression shows that in this case $\delta = n$.

We first show that any solution of (3) leads to a solution of (5). For this, let $\prod_{i=1}^k p_i$ be the radical of $\frac{X^n-1}{n^e(X-1)}$. Obviously, $\text{rad}(\frac{X^n-1}{n^e(X-1)}) | \text{rad}(X^n-1)$. Let $\zeta \in \mathbb{C}$ be a primitive n -th root of unity. Then the numbers $\alpha_c = \frac{X-\zeta^c}{(1-\zeta^e)^e} \in \mathbb{Z}[\zeta]$ by definition of e , and $(\alpha_c, n) = 1$. Since for distinct $c, d \not\equiv 0 \pmod n$ we have $(1-\zeta^d)^e \cdot \alpha_d - (1-\zeta^c)^e \cdot \alpha_c = \zeta^c - \zeta^d$, it follows that $(\alpha_c, \alpha_d) | (1-\zeta)$ and in view of $(\alpha_c, n) = 1$, it follows that the α_c are coprime.

Let $F = \prod_{c=1}^{n-1} \alpha_c = \frac{X^n-1}{n^e(X-1)}$ and $q | F$ be a rational prime. In the field $\mathbb{Q}[\zeta]$, it splits completely in the prime ideals $\mathfrak{Q}_c = (q, \alpha_c)$, $c = 1, 2, \dots, n-1$: these ideals are coprime, as a consequence of the coprimality of the α_c . Therefore $q \equiv 1 \pmod n$ and it follows from (1) that $(q, B) = 1$, so $q | Z$. Furthermore, (3) implies that there exists $j_q > 0$ such that $q^{j_q n} || Z^n$ and thus $q^{j_q n} || F$. This holds for all primes $q | \text{rad}(F)$. It follows that (5) is verified for $Y = \prod_{q|F} q^{j_q}$ and $Y | Z$. We have thus proved that if (X, Z) is a solution of (3) for the prime n , then there exists $C \in \mathbb{Z}$ such that $Z = C \cdot Y$ with Y as above, and:

$$(6) \quad \frac{X^n - 1}{n^e(X - 1)} = Y^n \quad \text{and}$$

$$(7) \quad X - 1 = B \cdot C^n / n^e.$$

We shall write from now on $D = X - 1$.

From the above, we conclude that any integer solution of (3) induces one of (5). Conversely, if (X, Y) is a solution of (5), then $(X, Y; n^e(X - 1))$ is a solution of (3). For instance, the particular solution $(X, Y; B) = (18, 7; 17)$ of (3) stems from

$$\frac{18^3 - 1}{18 - 1} = 7^3,$$

which is supposed to be the only non trivial solution of (5).

Remark 2.1. Note that if (X, Z) verify (3), then $(-X, Z)$ is a solution of $\frac{X^n+1}{X+1} = BZ^n$, so the results apply also to the equation:

$$X^n + 1 = BZ^n.$$

2.2. Bounds to the solutions of Equation (5). We shall use the following Theorem from [Mi2]:

Theorem 2.2. Suppose that X, Y are integers verifying (5) with $n \geq 17$ being a prime. Let $u = (X \pmod n)$. Then there is an $E \in \mathbb{R}_+$ such that $|X| < E$. The values of E in the various cases of the equation are the following:

$$(8) \quad E = \begin{cases} 4 \cdot \left(\frac{n-3}{2}\right)^{\frac{n+2}{2}} & \text{if } u \notin \{-1, 0, 1\} \\ (4n)^{\frac{n-1}{2}} & \text{if } u = 0, \\ 4 \cdot (n-2)^n & \text{otherwise.} \end{cases}$$

By comparing the bounds (8) with (7), it follows that $|C| < 2n - 1$. In particular, the primes dividing C do not split completely in $\mathbb{Q}[\zeta_n]$ – since a prime splitting in this field has the form $r = 2kn + 1 > 2n$.

Remark 2.3. Note that $|C| < 2n - 1$ implies a fortiori that for all primes $r|C$, $r^2 \not\equiv 1 \pmod n$. If $d(r) \leq \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ is the decomposition group of the unramified prime r , it follows that $|d(r)| \geq 3$; moreover, either $d(r)$ contains a subcycle $d' \subset d(r)$ of odd order $|d'| \geq 3$ or it is a cyclic 2-group with at least 4 elements.

2.3. A combinatorial lemma.

Lemma 2.4. Let p be an odd prime, $k \in \mathbb{N}$ with $1 < k < \log_2(p)$ and $P = \{1, 2, \dots, p-1\}$. If $S = \{a_1, a_2, \dots, a_k\} \subset P$ be a set of numbers coprime to p and such that $a_i \not\equiv \pm a_j \pmod p$ for $i \neq j$. We set the bound $A = 2\lceil p^{1/k} \rceil$; then there are k numbers $b_i \in \mathbb{Z}$, $i = 1, 2, \dots, k$, not all zero, with $0 \leq |b_i| \leq A$ and such that

$$\sum_{i=1}^k a_i b_i \equiv 0 \pmod p.$$

For $k = 2$, we can choose the b_i such that the additional condition

$$\sum_{i=1}^2 b_i/a_i \not\equiv 0 \pmod p.$$

holds.

Proof. Let $T = \{1, 2, \dots, A\} \subset P$. Consider the functional $f : T^k \rightarrow \mathbb{Z}/(p \cdot \mathbb{Z})$ given by

$$f(\vec{t}) \equiv \sum_{i=1}^k t_i a_i \pmod p, \quad \text{with } \vec{t} = (t_1, t_2, \dots, t_k) \in T^k.$$

Since $|T^k| > p$, by the pigeon hole principle there are two vectors $\vec{t} \neq \vec{t}'$ such that $f(\vec{t}) \equiv f(\vec{t}') \pmod p$. Let $b_i = t_i - t'_i$; by construction, $0 \leq |b_i| \leq A$ and not all b_i are zero, since $\vec{t} \neq \vec{t}'$. The choice of these vectors implies $\sum_{i=1}^k a_i b_i \equiv 0 \pmod p$, as claimed.

We now turn to the second claim. If the claim were false, then

$$a_1 b_1 + a_2 b_2 = 0 \text{ and } b_1/a_1 + b_2/a_2 = 0,$$

a homogenous linear system S with determinant $\det(S) = \frac{a_1^2 - a_2^2}{a_1 a_2}$, which is non vanishing under the premise of the lemma. This would imply that the solution b_1, b_2 is trivial, in contradiction with our construction. This completes the proof. \square

2.4. Some notation. We assume that n is prime and let ζ be a primitive n -th root of unity, $\mathbb{K} = \mathbb{Q}(\zeta)$ the n -th cyclotomic field and $G = \text{Gal}(\mathbb{K}/\mathbb{Q})$ the Galois group. The automorphisms $\sigma_a \in G$ are given by $\zeta \mapsto \zeta^a$, $a = 1, 2, \dots, n-1$; complex conjugation is denoted by $j \in \mathbb{Z}[G]$. In the ring of integers $\mathbb{Z}[\zeta]$, one has finite λ -adic expansions: for any $\alpha \in \mathbb{Z}[\zeta]$ and some $N > 0$ there are $a_j \in \{-(p-1)/2, \dots, 0, 1, \dots, (p-3)/2\}$, $j = 0, 1, \dots, N$ such that:

$$(9) \quad \alpha = \sum_{j=0}^N a_j (1 - \zeta)^j.$$

We shall use the algebraic $O(\cdot)$ -notation, to suggest the remainder of a power series. This occurs explicitly in the following four contexts

- (i) In a λ -adic development of the type (9), we write $\alpha = x + O(\lambda^m)$ to mean that there is some $y \in \mathbb{Z}[\zeta]$ such that $\alpha - x = \lambda^m y$. Since $(n) = (\lambda^{p-1})$, powers of n can occur as well as powers of λ in this notation.

- (ii) We also use formal power series, often written $f = f(D) \in \mathbb{K}[[D]]$. For $f = \sum_{k=0}^{\infty} f_k D^k$ with partial sum $S_m(f) = \sum_{k=0}^m f_k D^k$ we may also use the $O(\cdot)$ -notation and denote the remainder by $f(D) = S_m(D) + O(D^{m+1})$.
- (iii) Suppose that D is an integer and the formal power series converges in the completion $\mathbb{K}_{\mathfrak{P}}$ at some prime $\mathfrak{P} \subset \mathcal{O}(\mathbb{K})$ dividing D . Suppose also that in this case all coefficients of f be integral: then the remainder $f(D) - S_m(D)$ is by definition divisible by \mathfrak{P}^{m+1} , so $O(D^{m+1})$ means in this context that the remainder is divisible by \mathfrak{P}^{m+1} .
- (iv) If $f(D)$ converges at all the prime ideals dividing some integer $a|D$, then $O(D^{m+1})$ will denote a number divisible by a^{m+1} . In this paper we shall use this fact in the context in which $a = p$ is an integer prime dividing D and such that $f(D)$ converges at all prime ideals of \mathbb{K} above p .

2.5. Auxiliary facts on the Stickelberger module. The following results are deduced in [Mi2], Section 4, but see also [Mi1], §2.1-2.3 and §4.1. The results shall only be mentioned here without proof.

The Stickelberger module is $I = (\vartheta \cdot \mathbb{Z}[G]) \cap \mathbb{Z}[G]$, where $\vartheta = \frac{1}{n} \sum_{c=1}^{n-1} c \cdot \sigma_c^{-1}$ is the Stickelberger element. For $\theta = \sum_c n_c \sigma_c \in I$ we have the relation $\theta + j\theta = \varsigma(\theta) \cdot \mathbf{N}$, where $\varsigma(\theta) \in \mathbb{Z}$ is called the *relative weight* of θ . The augmentation of θ is then

$$|\theta| = \sum_c n_c = \varsigma(\theta) \cdot \frac{n-1}{2}.$$

The Fueter elements are

$$\psi_k = (1 + \sigma_k - \sigma_{k+1}) \cdot \vartheta = \sum_{c=1}^{n-1} \left(\left\lfloor \frac{(k+1)c}{n} \right\rfloor - \left\lfloor \frac{kc}{n} \right\rfloor \right) \cdot \sigma_c^{-1}, \quad 1 \leq k \leq (n-1)/2.$$

Together with the norm, they generate I as a \mathbb{Z} -module (of rank $(n+1)/2$) and $\varsigma(\psi_k) = 1$ for all k .

The Fuchsian elements are

$$\Theta_k = (k - \sigma_k) \cdot \vartheta = \sum_{c=1}^{n-1} \left\lfloor \frac{kc}{n} \right\rfloor \cdot \sigma_c^{-1}, \quad 2 \leq k \leq n.$$

They also generate I as a \mathbb{Z} -module. Note that Θ_n is the norm, and that we have the following relationship between the Fueter and the Fuchsian elements:

$$\psi_1 = \Theta_2 \text{ and } \psi_k = \Theta_{k+1} - \Theta_k, \quad k \geq 2$$

An element $\Theta = \sum_c n_c \sigma_c$ is *positive* if $n_c \geq 0$ for all $c \in \{1, 2, \dots, p-1\}$. We write $I^+ \subset I$ for the set of all positive elements. They form a multiplicative and an additive semigroup.

The Fermat quotient map $I \rightarrow \mathbb{Z}/(n \cdot \mathbb{Z})$, given by

$$\varphi : \theta = \sum_{c=1}^{n-1} n_c \sigma_c \mapsto \sum_{c=1}^{n-1} c n_c \bmod n,$$

is a linear functional, with kernel $I_f = \{\theta \in I : \zeta^\theta = 1\}$ (the *Fermat module*), and enjoys the properties:

$$\begin{aligned}\zeta^\theta &= \zeta^{\varphi(\theta)}, \\ (1 + \zeta)^\theta &= \zeta^{\varphi(\theta)/2}, \\ (1 - \zeta)^\theta &= \zeta^{\varphi(\theta)/2} \cdot \left(\left(\frac{-1}{n} \right) n \right)^{\varsigma(\theta)/2},\end{aligned}$$

where $\left(\frac{-1}{n} \right)$ is the Legendre symbol.

The last relation holds up to a sign which depends on the embedding of ζ . For a fixed embedding, we let $\nu = \sqrt{\left(\frac{-1}{n} \right) n}$ be the generator of the quadratic subfield $\mathbb{Q}(\nu) \subset \mathbb{Q}(\zeta)$. A short computation shows that $(1 - \zeta)^\theta = \zeta^{\varphi(\theta)/2} \nu$. Note that for $\theta \in I$ with $\varsigma(\theta) = 2$ we have $(1 - \zeta)^{2\theta} = \zeta^{\varphi(\theta)} \cdot n^2$ for any embedding.

We shall want to consider the action of elements of $\theta \in \mathbb{F}_n[G]$ on explicit algebraic numbers $\beta \in \mathbb{K}$. Unless otherwise specified, an element $\theta = \sum_{c=1}^{n-1} m_c \sigma_c \in \mathbb{F}_n[G]$ is lifted to $\sum_{c=1}^{n-1} n_c \sigma_c$, where $n_c \in \mathbb{Z}$ are the unique integers with $0 \leq n_c < p$ and $n_c \equiv m_c \pmod{p}$. In particular, lifts are always positive, of bounded weight $w(\theta) \leq (p-1)^2$. Rather than introducing an additional notation for the lift defined herewith, we shall always assume, unless otherwise specified, that $\theta \in \mathbb{F}_p[G]$ acts upon $\beta \in \mathbb{K}$ via this lift.

Using this lift, we define the following additive maps:

$$\rho_0 : \mathbb{F}_n[G] \rightarrow \mathbb{Q}(\zeta) \quad \theta = \sum_{c=1}^{n-1} n_c \sigma_c \mapsto \sum_{c \in P} \frac{n_c}{1 - \zeta^c},$$

and

$$\rho : \mathbb{F}_n[G] \rightarrow \mathbb{Z}[\zeta] \quad \theta \mapsto (1 - \zeta) \cdot \rho_0[\theta].$$

The i -th moment of an element $\theta = \sum_{c=1}^{n-1} n_c \sigma_c$ of $\mathbb{Z}[G]$ is defined as:

$$\phi^{(i)}(\theta) = \sum_{c=1}^{n-1} n_c c^i \pmod{n}.$$

Note that $\phi^{(1)}$ is the *Fermat quotient map*: $\phi^{(1)} = \varphi$. The moments are linear maps of \mathbb{F}_p -vector spaces and homomorphism of algebras, verifying:

$$(10) \quad \begin{aligned} \phi^{(i)}(a\theta_1 + b\theta_2) &= a\phi^{(i)}(\theta_1) + b\phi^{(i)}(\theta_2), \quad \text{and} \\ \phi^{(i)}(\theta_1\theta_2) &= \phi^{(i)}(\theta_1)\phi^{(i)}(\theta_2), \quad \text{with } \theta_j \in \mathbb{F}_p[G]; a, b \in \mathbb{F}_p. \end{aligned}$$

The linearity in the first identity is a straight-forward verification from the definition. For the second, note that for $\theta = \sum_c n_c \sigma_c$ we have

$$\phi^{(i)}(\sigma_a \theta) = \phi^{(i)}\left(\sum_c n_c \sigma_{ac}\right) = \sum_c n_c \cdot (ac)^i = a^i \cdot \phi^{(i)}(\theta).$$

Using the already established linearity, one deduces the multiplicativity of $\phi^{(i)}$ as a ring homomorphism.

Let $\alpha = \frac{X - \zeta}{(1 - \zeta)^e} \in \mathbb{Z}[\zeta]$, as before, and define $c_X \equiv 1/(X - 1) \pmod{n}$ if $e = 0$ and $c_X = 0$ if $e = 1$. For any $\theta \in I^+$, there is a *Jacobi integer* $\beta[\theta] \in \mathbb{Z}[\zeta]$ such

that $\beta[\theta]^n = (\zeta^{c_X} \alpha)^\theta$, normed by $\beta[\theta] \equiv 1 \pmod{(1-\zeta)^2}$ (Lemma 2 of [Mi2]). The definition of $\varsigma(\theta)$ implies that

$$(11) \quad \beta[\theta] \cdot \overline{\beta[\theta]} = \mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\alpha)^{\varsigma(\theta)} = Y^{\varsigma(\theta)}.$$

We have for any $\theta \in I^+$,

$$(12) \quad \beta[\theta]^n = (\zeta^{c_X} \alpha)^\theta = (\zeta^{c_X} (1-\zeta)^{1-e})^\theta \cdot \left(1 + \frac{X-1}{1-\zeta}\right)^\theta$$

Lemma 2.5. *We remind that $D = X - 1$. For any $\theta \in 2 \cdot I_f^+$, for any prime ideal $\mathfrak{P} \mid D$, there is a $\kappa = \kappa_{\mathfrak{P}}(\theta) \in \mathbb{Z}/(n \cdot \mathbb{Z})$ such that*

$$\beta[\theta] \equiv \zeta^\kappa \cdot Y^{\frac{\varsigma(\theta)}{2}} \pmod{\mathfrak{P}}.$$

Proof. Let θ_0 be an element of I_f^+ , and let $\theta = 2\theta_0$. Note that from (11) we have $Y^{\varsigma(\theta_0)n} = \beta[\theta_0]^n \cdot \overline{\beta[\theta_0]}^n$. Thus $\beta[\theta]^n = \beta[\theta_0]^{2n} = Y^{\varsigma(\theta_0)n} \cdot (\beta[\theta_0]/\overline{\beta[\theta_0]})^n$. Using (12) and the previous observations, we find:

$$\begin{aligned} \beta[\theta]^n &= Y^{\varsigma(\theta_0)n} \cdot (\zeta^{c_X} \cdot (1-\zeta)^{1-e})^{(\theta_0 - j\theta_0)} \cdot \left(1 + \frac{X-1}{1-\zeta}\right)^{(\theta_0 - j\theta_0)} \\ &= Y^{\varsigma(\theta_0)n} \cdot \zeta^{(2c_X+1)\varphi(\theta_0)} \cdot (1 + D/(1-\zeta))^{(\theta_0 - j\theta_0)} \\ (13) \quad \beta[\theta]^n &= Y^{\varsigma(\theta_0)n} \cdot \left(1 + \frac{D}{1-\zeta}\right)^{(\theta_0 - j\theta_0)}. \end{aligned}$$

Thus for any prime ideal $\mathfrak{P} \mid D$ there is a $\kappa = \kappa_{\mathfrak{P}}(\theta) \in \mathbb{Z}/(n \cdot \mathbb{Z})$ such that

$$(14) \quad \beta[\theta] \equiv \zeta^\kappa \cdot Y^{\varsigma(\theta_0)} \pmod{\mathfrak{P}}.$$

□

In the sequel, we indicate how to choose θ such that $\kappa = 0$. In this case, the relation (12) leads to a \mathfrak{P} -adic binomial series expansion for $\beta[\theta]$.

We will use the Voronoi identities – see Lemma 1.0 in [Jha] –, which we remind here for convenience:

Lemma 2.6. *Let m be an even integer such that $2 \leq m \leq n-1$. Let a be an integer, coprime to n . Then*

$$(15) \quad a^m \sum_{j=1}^{n-1} \left[\frac{aj}{n} \right] j^{m-1} \equiv \frac{(a^{m+1} - a)B_m}{m} \pmod{n},$$

where B_m is the m -th Bernoulli number. In particular, for $m = n-1$, we get

$$\sum_{j=1}^{n-1} \left[\frac{aj}{n} \right] j^{n-2} \equiv \frac{a^n - a}{n} \pmod{n},$$

which is the Fermat quotient map of the a -th Fuchsian element, $\varphi(\Theta_a)$.

Lemma 2.7. *Let ψ_k denote the k -th Fueter element. Then, there exists a linear combination $\theta = \sigma\psi_k + \tau\psi_l \in I$ with $\sigma, \tau \in G$ and $1 \leq k, l < n$ such that $\phi^{(1)}(\theta) = 0$ and $\phi^{(-1)}(\theta) \neq 0$.*

The proof of this Lemma is elementary, using the Voronoi relations (15); since the details are rather lengthy, they will be given in the Appendix.

The following two lemmata contain computational information for binomial series developments that we shall use below. First, we remind that ρ_0 is the following additive map:

$$\rho_0 : \mathbb{F}_n[G] \rightarrow \mathbb{Q}(\zeta) \quad \theta = \sum_{c=1}^{n-1} n_c \sigma_c \mapsto \sum_{c \in P} \frac{n_c}{1 - \zeta^c}$$

Lemma 2.8. *Let D be an indeterminate. Let $\theta = \sum_{c=1}^{n-1} n_c \sigma_c \in \mathbb{Z}[G]$ and $f[\theta] = \left(1 + \frac{D}{1-\zeta}\right)^{\theta/n} \in \mathbb{K}[[D]]$. Let $0 < N < n$ be a fixed integer. Then,*

$$f[\theta] = 1 + \sum_{k=1}^N \frac{a_k[\theta]}{k!n^k} D^k + O(D^{N+1}),$$

where, for $1 \leq k \leq N$, we have

$$a_k[\theta] = \rho_0^k[\theta] + O\left(\frac{n}{(1-\zeta)^k}\right).$$

In the above identity, $a_k[\theta], \rho_0^k[\theta] \in \mathbb{Z}[\zeta, \frac{1}{n}]$ are not integral, but their difference is an algebraic integer $a_k[\theta] - \rho_0^k[\theta] \in \frac{n}{(1-\zeta)^k} \cdot \mathbb{Z}[\zeta]$.

Proof. Let $\theta = \sum_c n_c \sigma_c$ and $m = m(\theta) = |\{c : n_c \neq 0\}|$ be the number of non vanishing coefficients of θ . We prove this result by induction on m . First, note that

$$\binom{n_c/n}{k} = \frac{1}{k!} \cdot \frac{n_c^k}{n^k} \cdot (1 + O(n)).$$

Thus, if $\theta = n_c \sigma_c$ and $m = 1$, then:

$$f[\theta] = 1 + \sum_{k=1}^{n-1} \frac{1}{k!} \cdot \frac{n_c^k}{n^k} \cdot (1 + O(n)) \cdot \frac{D^k}{(1-\zeta)^k} = 1 + \sum_{k=1}^N \frac{a_k[\theta]}{k!n^k} D^k + O(D^{N+1}),$$

where, for $1 \leq k \leq N$,

$$a_k[\theta] = \rho_0^k[\theta] + O\left(\frac{n}{(1-\zeta)^k}\right),$$

which confirms the claim for $m = 1$. Suppose the claim holds for all $j \leq m$ and let $\theta = \theta_1 + \theta_2$ with $m(\theta_i) < m$ and $m(\theta) = m$. Then,

$$\begin{aligned} f[\theta] &= \left(1 + \frac{D}{1-\zeta}\right)^{\theta_1/n} \cdot \left(1 + \frac{D}{1-\zeta}\right)^{\theta_2/n} \\ &= 1 + \sum_{k=1}^N \alpha_k[\theta] D^k + O(D^{N+1}), \end{aligned}$$

where for $k < n - 1$ we have

$$\begin{aligned} \alpha_k[\theta] &= \sum_{j=1}^k \frac{a_j[\theta_1]}{n^j j! (1-\zeta)^j} \cdot \frac{a_{k-j}[\theta_2]}{n^{k-j} (k-j)! (1-\zeta)^{k-j}} \cdot (1 + O(n)) \\ &= \frac{1}{k!n^k} (\rho_0[\theta_1] + \rho_0[\theta_2])^k + O\left(\frac{n}{k!n^k (1-\zeta)^k}\right) \\ &= \frac{1}{k!n^k} \cdot \rho_0^k[\theta] + O\left(\frac{n}{k!n^k (1-\zeta)^k}\right) = \frac{1}{k!n^k} \cdot (\rho_0^k[\theta] + O(n/(1-\zeta)^k)) \end{aligned}$$

This proves the claim by complete induction. \square

Lemma 2.9. *By proceeding like in Lema 8 of [Mil], we notice that $\frac{a_k[\theta]}{k!} \in \mathbb{Z}[\zeta]$ (notation is different between both articles).*

As a consequence, we may deduce that matrices built from the first coefficients occurring in some binary series developments are regular.

Lemma 2.10. *Let $\theta = \sum_{c=1}^{n-1} n_c \sigma_c \in \mathbb{Z}[G]$ such that $\phi^{(-1)}(\theta) \not\equiv 0 \pmod n$, let $f[\theta] = \left(1 + \frac{D}{1-\zeta}\right)^{\theta/n}$ and $0 < N < n-1$ be a fixed integer. Then,*

$$f[\theta] = 1 + \sum_{k=1}^N \frac{b_k[\theta]}{k!n^k(1-\zeta)^k} D^k + O(D^{N+1}), \quad \text{with } \frac{b_k[\theta]}{k!} \in \mathbb{Z}[\zeta].$$

Moreover, if $J \subset \text{Gal}(\mathbb{Q}[\zeta]/\mathbb{Q})$ is a subset with $|J| = N$, then the matrix¹

$$A_N = (b_k[\sigma_c \theta])_{k=0; \sigma_c \in J}^{N-1} \in GL(\mathbb{K}, N)$$

Proof. Let $\lambda = 1 - \zeta$; we show that the determinant of A_N is not zero modulo λ . Using Lemma 2.8, we know that we have a development of symbolic power series

$$f[\theta] = 1 + \sum_{k=1}^N \frac{a_k[\theta]}{k!n^k} D^k + O(D^{N+1}),$$

where

$$a_k[\theta] = \rho_0^k[\theta] + O\left(\frac{n}{(1-\zeta)^k}\right).$$

By definition, $(1-\zeta)^k \cdot a_k[\sigma_c \theta] \in \mathbb{Z}[\zeta]$ for all $\sigma_c \in G$. Let $b_k[\theta] = (1-\zeta)^k \cdot a_k[\theta] \in \mathbb{Z}[\zeta]$. Then, according to Lemma 2.8,

$$\begin{aligned} b_k[\sigma_c \theta] &= (1-\zeta)^k \cdot \left(\rho_0^k[\sigma_c \theta] + O\left(\frac{n}{(1-\zeta)^k}\right) \right) \\ &= \rho^k[\sigma_c \theta] + O(n) = \left(\sum_{l=1}^{n-1} n_l \cdot \frac{1-\zeta}{1-\zeta^{lc}} \right)^k + O(n) \\ &\equiv \left(\sum_{l=1}^{n-1} \frac{n_l}{lc} \right)^k \pmod{\lambda} \equiv \left(\frac{\phi^{(-1)}[\theta]}{c} \right)^k \pmod{\lambda}. \end{aligned}$$

Thus, $\det A_N \equiv \left| \left(\left(\frac{\phi^{(-1)}[\theta]}{c} \right)^k \right)_{k=0, \sigma_c \in J}^{N-1} \right| \pmod{\lambda}$. We have obtained a Vandermonde determinant:

$$\det A_N \equiv \left(\phi^{(-1)}[\theta] \right)^{N(N-1)/2} \cdot \prod_{i \neq j; \sigma_i, \sigma_j \in J} \left(\frac{1}{i} - \frac{1}{j} \right) \pmod{\lambda}.$$

By hypothesis, $\phi^{(-1)}[\theta] \not\equiv 0 \pmod n$, and $1/i \not\equiv 1/j \pmod n$ for $\sigma_i, \sigma_j \in J$; this implies finally that $\prod_{\sigma_i, \sigma_j \in J} \left(\frac{1}{i} - \frac{1}{j} \right) \not\equiv 0 \pmod n$, which confirms our claim. \square

¹We shall apply this Lemma below, in a context in which J satisfies the additional condition that $i+j \neq n$ for any i, j with $\sigma_i \in J$ and $\sigma_j \in J$.

3. PROOF OF THEOREM 1.2

Theorem 4 in [Mi2] proves that if CF holds, then (5) has no solution except for (8). The computations in [BH] prove that CF holds for $n \leq 163 \cdot 10^6$. This proves Theorem 1.2.(A). Theorem 1.2.(C) is also proved in Theorem 4 in [Mi2]. In the sequel we shall show that the only possible solutions are $X = \pm B/n^e + 1$. We may assume in particular that $n > 163 \cdot 10^6$.

We have already proved that $X - 1 = B \cdot C^n / n^e$. If $C = \pm 1$, then $X - 1 = \pm B/n^e$, as stated in point (B) of Theorem 1.2 and X is a solution of (5). The bounds on $|X|$ in (8) imply $|B| < n^n$, the second claim of (B).

Consequently, Theorem 3 will follow if we prove that $C = \pm 1$; we do this in this section. Assume that there is a prime $p|C$ with $p^i \nmid C$. Let $\mathfrak{P} \subset \mathbb{Z}[\zeta]$ be a prime ideal lying above p and let $d(p) \subset G$ be its decomposition group. We shall use Remark 2.3 in order to derive some group ring elements which cancel the exponents κ occurring in (14).

Recall that $D = B \cdot C^n / n^e = X - 1$, with C defined by (7). Note that (7) implies that either $(n, D) = 1$, or $n^2|B$ and $(n, C) = 1$. Indeed, if $(n, D) \neq 1$, then $e = 1$ and $n^2|n^e(X - 1) = BC^n$ and since $(C, n) = 1$, it follows that $n^2|B$; the last relation follows from the bounds $C^n \leq E < 4(n - 2)^n$, hence $|C| < n$. In both cases $1/(1 - \zeta)$ is congruent to an algebraic integer modulo $D/n^{v_n(D)} \cdot \mathbb{Z}[\zeta]$.

According to Remark 2.3, we know that there are at least two elements, $\sigma'_1, \sigma'_2 \in d(p)$ such that $\sigma'_1 \neq j \cdot \sigma'_2$. Let $\sigma'_i(\zeta) = \zeta^{c_i}$, $c_i \in (\mathbb{Z}/n \cdot \mathbb{Z})^*$. It follows from Lemma 2.4 that, for $c_i \neq c_j$ when $i \neq j$, there are $h'_1, h'_2 \in \mathbb{Z}$ with $|h'_i| \leq \sqrt{n}$ and $\sum_{i=1}^2 h'_i c_i \equiv 0 \pmod{n}$ while $\sum_{i=1}^2 h'_i / c_i \not\equiv 0 \pmod{n}$.

We define

$$(16) \quad \begin{aligned} \mu &= \sum_{i=1}^2 h_i \sigma_i \in \mathbb{Z}[d(p)] \subset \mathbb{Z}[G], \quad \text{with} \\ h_i &= \begin{cases} h'_i & \text{if } h'_i > 0 \text{ and} \\ -h'_i & \text{otherwise,} \end{cases} \quad \text{and} \\ \sigma_i &= \begin{cases} \sigma'_i & \text{if } h'_i > 0 \text{ and} \\ j\sigma'_i & \text{otherwise.} \end{cases} \end{aligned}$$

By construction, μ is a positive element, i.e. the coefficients $h_i \geq 0$. Let $\widehat{\cdot} : G \rightarrow (\mathbb{Z}/n \cdot \mathbb{Z})^*$ denote the cyclotomic character and note that $h'_i \widehat{\sigma} = h_i \widehat{\sigma'}$ for $h'_i < 0$ and thus $\phi^{(1)}(\mu) = 0$. In view of Lemma 2.4, we also know that we can choose the h'_i and thus μ , such that

$$\phi^{(1)}(\mu) = 0, \quad \text{but} \quad \phi^{(-1)}(\mu) \neq 0.$$

Since \mathbb{K}/\mathbb{Q} is abelian, all the primes $\mathfrak{P}(p)$ have the same decomposition group $d(p)$ and μ enjoys the following stronger property: let $\mathfrak{P}(p)$ and $S \subset G$ be a set of representatives of $G/d(p)$; let $\gamma \in \mathbb{Z}[\zeta]$ be such that $\gamma \equiv \zeta^{c_\sigma} \pmod{\sigma(\mathfrak{P})}$ for all $\sigma \in S$; then $\gamma^\mu \equiv 1 \pmod{p\mathbb{Z}[\zeta]}$, as follows directly from $\zeta^\mu \equiv 1 \pmod{\sigma(\mathfrak{P})}$, for all $\sigma \in S$.

In view of Lemma 2.7 and the fact that Fueter elements are positive, we also know that there is a $\theta_0 \in I_f^+$ such that $\varsigma(\theta_0) = 2$ and $\phi^{(-1)}(\theta_0) \neq 0$.

Let

$$\Theta = 2 \cdot \mu \cdot \theta_0.$$

In view of the properties (10) of moments and since for both μ, θ_0 , the Fermat quotient vanishes, while $\phi^{(-1)}$ is non-null, it follows that the same must hold for Θ ,

so $\Theta \in 2 \cdot I_f^+$ and $\phi^{(-1)}(\Theta) \neq 0$. Let

$$h = 2 \cdot \sum_{i=1}^l |h_i| = 2 \cdot w(\mu),$$

where we defined the *absolute weight* $w(\sum_c n_c \sigma_c) = \sum_c |n_c|$. From subsection 2.5, we know that there exists a Jacobi integer $\beta[2\theta_0] \in \mathbb{Z}[\zeta]$ such that $\beta[2\theta_0]^n = (\zeta^{c_X}(1-\zeta)^{1-\epsilon})^{\theta_0} \cdot \left(1 + \frac{X-1}{1-\zeta}\right)^{\theta_0}$ (see (12)). It follows from (2.5) and Lemma 2.5, that in both cases we have $\beta[2\theta_0] \equiv \zeta^{\kappa(\theta_0)} \cdot Y^4 \pmod{\mathfrak{P}}$. We have chosen μ as a linear combination of two elements from the decomposition group $D(\mathfrak{P}) \subset G$, so μ acts on $\zeta \pmod{\mathfrak{P}}$ by $\zeta \pmod{\mathfrak{P}} \mapsto \zeta^\mu \equiv 1 \pmod{\mathfrak{P}}$. Therefore, from $\beta[\Theta] = \beta[2\theta_0]^\mu$ and thus, by the choice of μ , we have

$$(17) \quad \beta[\Theta] \equiv Y^h \pmod{p\mathbb{Z}[\zeta]}.$$

Let $\Theta = 2 \sum_{c=1}^{n-1} n_c \sigma_c$; for any prime $\mathfrak{P} \mid (p)$, the binomial series of the n -th root of the right hand side in (13) converges in the \mathfrak{P} -adic valuation and its sum is equal to $\beta[\Theta]$ up to a possible n -th root of unity ζ^c . Here we make use of the choice of Θ : comparing (17) with the product above, it follows that $\zeta^c = 1$ for all primes $\mathfrak{P} \mid (p)$. For any $N > 0$, we have $p^{inN} \mid D^N$ and thus

$$(18) \quad \beta[\Theta] \equiv Y^h \prod_{c=1}^{n-1} \left(\sum_{k=0}^{N-1} \binom{n_c/n}{k} \left(\frac{D}{1-\zeta^c} \right)^k \right) \pmod{p^{inN}}.$$

We develop the product in a series, obtaining an expansion which converges uniformly at primes above p and is Galois covariant; for $N < n-1$ and $\sigma \in G$, we have:

$$\beta[\sigma\Theta] = Y^h \left(1 + \sum_{k=1}^{N-1} \frac{b_k[\sigma\Theta]}{(1-\zeta)^k n^k k!} \cdot D^k \right) + O(p^{inN}),$$

with $b_k[\Theta] \in \mathbb{Z}[\zeta]$. Let $P \subset \{1, 2, \dots, n-1\}$ be a set of cardinal $1 < N < (n-1)/2$ such that if $c \in P$ then $n-c \notin P$, and $J \subset \mathbb{Z}[G]$ be the Galois automorphisms of \mathbb{K} indexed by P : $J = \{\sigma_c\}_{c \in P}$. Consider the linear combination $\Delta = \sum_{\sigma \in J} \lambda_\sigma \cdot \beta[\sigma \cdot \Theta]$ where $\lambda_\sigma \in \mathbb{Q}[\zeta]$ verify the linear system:

$$(19) \quad \begin{aligned} \sum_{\sigma \in J} \lambda_\sigma \cdot b_k[\sigma \cdot \Theta] &= 0, \text{ for } k = 0, \dots, N-1, \ k \neq \lceil N/2 \rceil \quad \text{and} \\ \sum_{\sigma \in J} \lambda_\sigma \cdot b_{\lceil N/2 \rceil}[\sigma \cdot \Theta] &= (1-\zeta)^{\lceil N/2 \rceil} n^{\lceil N/2 \rceil} \lceil N/2 \rceil!. \end{aligned}$$

Applying Lemma 2.8 we observe that this system is regular for any $N < n-1$. There exists therefore a unique solution which is not null.

We recall that a power series $\sum_{k=0}^{\infty} a_k X^k \in \mathbb{C}[[X]]$ is dominated by the series $\sum_{k=0}^{\infty} b_k X^k \in \mathbb{R}[[X]]$ with non-negative coefficients, if for all $k \geq 0$, we have $|a_k| \leq b_k$. The dominance relation is preserved by addition and multiplication of power series.

Following the proof of Proposition 8.2.1 in [Bilu], one shows that if $r \in \mathbb{R}_{>0}$ and $\chi \in \mathbb{C}$, with $|\chi| \leq K$ with $K \in \mathbb{R}_{>0}$, then the binomial series $(1 + \chi T)^r$ is dominated by $(1 - KT)^{-r}$. From this, we obtain that $(1 + \chi T)^{\Theta/n}$ is dominated by

$(1 - KT)^{-w(\Theta)/n}$. In our case (18), $T = D$, $\chi = \frac{1}{1-\zeta^c}$ and

$$K = \max_{1 \leq c < n} |1/(1 - \zeta^c)| = 1/\sin(\pi/n) \leq n/\pi \cos(\pi/3) = 2n/\pi < n.$$

Applying this to our selected Θ , whose absolute weight is bounded by $w \leq 4n\sqrt{n}$, we find after some computations that $|b_k[\sigma \cdot \Theta]| < n^k \cdot \binom{-w/n}{k} \cdot k! < n^{3k}$ for $N < n/2$.

Let $A = \det(b_k[\sigma_c \cdot \Theta])_{k=0; c \in I}^{N-1} \neq 0$ be the determinant of the matrix of the system (19), which is non vanishing, as noticed above: note that the division by $k!$ along a complete row does not modify the regularity of the matrix.

Let $\vec{d} = (1 - \zeta)^{\lceil N/2 \rceil} n^{\lceil N/2 \rceil} \lceil N/2 \rceil! (\delta_{k, \lceil N/2 \rceil})_{k=0}^{N-1}$, where $\delta_{i,j}$ is Kronecker's symbol. The solution to our system is $\lambda_\sigma = A_\sigma/A$, where $A_\sigma \in \mathbb{Z}[\zeta]$ are the determinants of some minors of $(b_k[\sigma_c \cdot \Theta])_{k=0; c \in I}^{N-1}$ obtained by replacing the respective column by \vec{d} .

Noticing that $|(1 - \zeta)^{\lceil N/2 \rceil} n^{\lceil N/2 \rceil} \lceil N/2 \rceil!| < n^{3(N-1)}$, Hadamard's inequality implies that

$$\begin{aligned} |A_\sigma| &\leq n^{3(N-1)(N-2)/2} \cdot (N-1)^{(N-1)/2} \leq n^{3N^2/2} \cdot N^{N/2} \quad \text{and} \\ |A| &\leq n^{3N^2/2} \cdot N^{N/2} \end{aligned}$$

Let $\delta = A \cdot \Delta \in \mathbb{Z}[\zeta]$,

$$\delta = \sum_{\sigma \in J} A_\sigma \cdot \beta[\sigma \cdot \Theta] \in \mathbb{Z}[\zeta].$$

We set $N = \lceil n^{3/4} \rceil$ and claim that for such N , $\delta \neq 0$. By choice of the λ 's, we have $\delta = A \cdot p^{in \lceil N/2 \rceil} \cdot u + p^{in N} z$ for some $z \in \mathbb{Z}[\zeta]$, where $u = \frac{D^{\lceil N/2 \rceil}}{p^{in \lceil N/2 \rceil}} \cdot Y^h$ is a unit in $(\mathbb{Z}/p\mathbb{Z})^*$. Therefore, if we assume that $\delta = 0$, then necessarily $p^{in \lceil N/2 \rceil}$ divides A . However, $v_p(A) < n \lceil N/2 \rceil$. Indeed, the upper bound for $|A|$ implies a fortiori that $v_p(A) \leq \lceil N/2 \cdot \log N + \frac{3N^2}{2} \log n \rceil$. Then, the assumption $\delta = 0$ would imply $n \leq 3 \lceil n^{3/4} + \frac{1}{4} \rceil \log n$, which is false for $n \geq 4, 5 \cdot 10^6$. This contradicts thus our initial assumption. Therefore $\delta \neq 0$.

Given the bounds on A_σ , we obtain $|\delta| \leq NY^h n^{3N^2/2} \cdot N^{N/2}$ and using the fact that $h < 4n^{1/2}$, $Y < n^n$ (Theorem 1.2.(B)) and $N = \lceil n^{3/4} \rceil$, we find

$$|\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta)| < \left(n^{\frac{11}{2}n^{3/2} + \frac{3}{8}n^{3/4} + \frac{3}{4}} \right)^{n-1}.$$

The initial homogenous conditions in (19) imply $\delta \equiv 0 \pmod{p^{in \lceil N/2 \rceil}}$, therefore $|\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta)| \geq p^{in(n-1)N/2}$. Combining this inequality with (20) and $n \geq 163 \cdot 10^6$, one finds that $\log p < 1.64$. This shows that $p = 2, 3$ or 5 .

We consider the case $p \leq 5$ separately as follows. We choose in this case $\mu = 1 + pJ\sigma_p^{-1}$ and verify that $\varphi(\mu) = 0$, while $\phi^{-1}(\mu) = 1 - p^2 \not\equiv 0 \pmod{n}$. Consequently $\varsigma(\Theta) = 4(p+1)$ and the norm of δ is thus bounded by

$$p^{n(n-1)N/2} \leq |\mathbf{N}_{\mathbb{K}/\mathbb{Q}}(\delta)| < \left(n^{4(p+1)+3N^2/2} \cdot N^{N/2+1} \right)^{n-1}.$$

Letting $N = 48$, we obtain the inequality

$$2^n \leq n^{73} \cdot 48^{25/24} < 64n^{73} \quad \Rightarrow \quad \frac{n-6}{73} \leq \log(n)/\log(2),$$

which is false for $n > 695$, and a fortiori for $n > 163 \cdot 10^6$. We obtain a contradiction in this case too, and thus $C = \pm 1$, which completes the proof of Theorem 1.2. \square

4. CONSEQUENCES FOR THE GENERAL CASE OF THE BINARY THUE EQUATION (3)

In this section we derive Theorem 1.3. For this we assume that (3) has a solution with $(\varphi^*(B), n) = 1$, since our results only hold in this case, a fact which is reflected also in the formulation of Theorem 1.3.

Consider the case when $n = p \cdot q$ is the product of two distinct primes. If $(n, B) = 1$, then Theorem 1.2 holds for both p and q with the value $e = 0$. If X, Z is a solution, then Theorem 1.2 . (B) implies that $X^p = \pm B + 1$ and $X^q = \pm B + 1$. Consequently either $X^p + X^q = 2$ or $X^p - X^q = 2$. This is impossible for $|X| > 2$ and a simple case distinction implies that there are no solutions. As a consequence,

Corollary 4.1. *Consider Equation (3) for fixed B and suppose that n is an integer which has two distinct prime divisors $p > q > 2$ with $(p, B) = (q, B) = 1$. Then (3) has no solutions for which (1) holds.*

If all divisors of n are among the primes dividing B , we are led to the following equation: $p(X^q - 1) = q(X^p - 1)$, which has no solutions in the integers other than 1. Indeed, assume $X \neq 1$ to be a solution of the previous equation, and $q = p + t$, $t \geq 0$. The real function $f(t) = p(X^{p+t} - 1) - (p + t)(X^p - 1)$ is strictly monotonous and $f(0) = 0$. Therefore, the equation $p(X^q - 1) = q(X^p - 1)$ has no solutions. There is only the case left in which n is built from two primes, one dividing B and one not. In this case, one obtains that equation $p(X^q - 1) = X^p - 1$ which can also be shown not to have non trivial solutions, using the above remark, this time with $f(t) = p(X^{p+t} - 1) - (X^p - 1)$. Hence:

Corollary 4.2. *The equation (3) has no solutions for exponents n which are divisible by more than one prime and for B such that (1) holds.*

We are left to consider the case of prime powers $n = p^c$ with $c > 1$. If $p \nmid B$, we obtain $X^{n/p} - 1 = B/p^e$, so in particular $B/p^e + 1 \geq 2^{p^{c-1}}$ is a p^{c-1} -th power. Since in this case, (3) has in particular a solution for the exponent p , the Theorem 1.2 implies that $B < p^p$; when $c > 2$, combining this with the previous lower bound implies that there are no solutions. For $c = 2$, we deduce that $|X| < p$ and, after applying the Theorem 1.2 again and letting $\xi = \zeta^{1/p}$ be a primitive p^2 -th root of unity, we obtain the equation

$$Y^{p^2} = \frac{X^{p^2} - 1}{p^e(X^p - 1)} = \mathbf{N}_{\mathbb{Q}[\xi]/\mathbb{Q}}(\alpha) \quad \alpha = \frac{X - \xi}{(1 - \xi)^e}.$$

As usual, the conjugates of the ideal (α) are pairwise coprime. We let $\mathfrak{A} = (Y, \alpha)$ be an ideal with $N(\mathfrak{A}) = (Y)$; moreover, if $\mathfrak{L}|\mathfrak{A}$ is a prime ideal and $N(\mathfrak{L}) = (\ell)$, then the rational prime ℓ is totally split in $\mathbb{Q}[\xi]$, the factors being the primes $(\ell, \sigma_c(\alpha))$. Being totally split, it follows in particular that $\ell \equiv 1 \pmod{p^2}$ so $Y \geq \ell > 2p^2$, in contradiction with $Y < X < p + 1$. This shows that there are no solutions for $n = p^2$. \square

Corollary 4.3. *If the Equation (3) in which $n = p^c$ is a prime power has non trivial solutions for which (1) holds, then $c = 1$.*

\square

The primes dividing the exponent n used in the above corollaries are by definition coprime to $\varphi^*(B)$. As a consequence, if n is an exponent for which (3) has a solution

and $m|n$ is the largest factor of n with $m \in \mathcal{N}(B)$ – as defined in (2) – then the corollaries imply that there is at most one prime dividing n/m and the exponent of this prime in the prime decomposition of n must be one. This is the first statement of Theorem 1.3, which thus follows from these corollaries and Theorem (3).

5. APPENDIX

The proof of Theorem 1.2 is based on results from [Mi2]. It has been pointed out that the proof of Theorem 3 in [Mi2] may require some more detailed explanation in the case of a singular system of equations in the proof of Lemma 14 of [Mi2]. Since the statements of [Mi2] are correct and can even be slightly improved, while the explanations may have seemed insufficient, we provide here for the readers interested to understand the technicalities of the proofs in [Mi2] some additional details and explanation, confirming those claims and results.

5.1. Clarification on the singular case of Theorem 3 in [Mi2]. Let $m \in \mathbb{Z}_{>0}$ be a positive integer, \mathbb{K} a field, $V = \mathbb{K}^m$ as a \mathbb{K} -vector space and let $L \subsetneq V$ be a proper subspace of V of dimension r . We assume that there exists at least one vector $w_1 \in L$ which is free of 0-coefficients over the canonical base \mathcal{E} . For $(x, y) \in V^2$, $x = (x_1, \dots, x_m)$ and $y = (y_1, \dots, y_m)$, the Hadamard product is defined by $[x, y] = (x_1 y_1, \dots, x_m y_m)$. For any subspace $W \subset V$ we define the W -bouquet of L by

$$L_W = \langle \{ [w, x] : w \in W, x \in L \} \rangle_{\mathbb{K}},$$

the \mathbb{K} -span of all the Hadamard products of elements in W by vectors from L .

Lemma 5.1. *Let $a_1 = (1, 1, \dots, 1)$ over \mathcal{E} , and $e_2 \in V$ such that its coordinates be pairwise distinct over \mathcal{E} . Let $A_2 = \langle \{a_1, a_2\} \rangle_{\mathbb{K}}$ be the subspace generated by e_1, e_2 . Let L_{A_2} be the resulting A_2 -bouquet. Then $\dim(L_{A_2}) > \dim(L)$.*

Proof. Obviously, $L \subset L_{A_2}$ (as $a_1 \in A$). We would like to show that $L_{A_2} \neq L$. We know that the system $(w_1, [w_1, a_2], [w_1, a_2^2], \dots, [w_1, a_2^{m-1}])$ (the notion of power of a vector here is to be understood as an “Hadamard power”) is free (as it induces a Vandermonde matrix over \mathcal{E} , w_1 does not have any zero among its coordinates and all coordinates of a_2 are pairwise distinct). We know that $w_1 \in L$; let us assume that $[w_1, a_2^j] \in L$ for $i \leq j$ (we know that $j \leq m - r < m$). Then, $[w_1, a_2^j] \in L$ and $[w_1, a_2^{j+1}] \notin L$. However, the Hadamard product of $[w_1, a_2^j] \in L$ by a_2 , that is $[w_1, a_2^{j+1}]$, belongs to L_{A_2} . Thus, $\dim L_{A_2} > \dim L$. \square

5.1.1. Application of Lemma 5.1 to the proof of the singular case in the argument on pages 266 – 270 of [Mi2]. We apply here the lemma in the first case (that is $x \not\equiv s \pmod{p}$, where $s \in \{-1, 0, 1\}$), the application to the second case being similar.

Let all notation be like in Lemma 14 in [Mi2]. As in [Mi2], we will assume that $\mathbf{A} = (\zeta^{-\kappa_{ac}/a})_{a,c=1}^{(p-1)/2}$ (where κ_{ac} are the *Galois exponents*) is singular. Let $m = (p-1)/2$, $\mathbb{K} = \mathbb{Q}(\zeta_p)$ and $r = \text{rank}(\mathbf{A}) < (p-1)/2$. Without loss of generality, we assume that a regular r -submatrix of \mathbf{A} is built with the first r rows and the first r columns. Therefore, the first r rows of \mathbf{A} are independent, and we denote by W the sub-space of $V = \mathbb{K}^m$ generated by the first r row vectors w_1, \dots, w_r of \mathbf{A} . For $a_1 = (1, 1, \dots, 1)$, we let a_2 be the vector of V whose components are ²

²In the context of [Mi2], η corresponds to $b_1[\theta]$ in our context

$(\eta(\sigma_c \theta))_{c=1}^{(p-1)/2}$ and $A_2 = \{a_1, a_2\}$. Then, according to Lemma 5.1, there exists at least one vector $\vec{v} \in L_{A_2}$ which is independent on the first r vectors of \mathbf{A} .

Let \mathbf{S} be the $(r+1) \times (r+1)$ submatrix of \mathbf{A} comprising the first r rows and $r+1$ columns of \mathbf{A} , to which we have added an additional row: the first $r+1$ components of \vec{v} . Let $\vec{\lambda}'$ be the vector solution of $\mathbf{A}\vec{\lambda}' = \vec{d}'$, where $\vec{d}' = (\delta_{c,r+1})_{c=1}^{r+1}$. We know that $\vec{\lambda}' \neq \vec{0}$, as \mathbf{S} is regular and \vec{d}' is not the null vector. For $1 \leq c \leq r+1$, by Cramer's rule, $\lambda_c = \frac{S_c}{S}$, where S_c are the determinants of some minors of \mathbf{S} obtained by replacing the c -column by \vec{d}' , and $S = \det \mathbf{S}$.

Let $\vec{\lambda} \in V$ be a vector whose first $r+1$ coordinates are those of $\vec{\lambda}'$ and the others are 0. Let $(\delta_{c,r+1})_{c=1}^m$. Then, $\vec{\lambda}$ verifies: $\mathbf{A}\vec{\lambda} = \vec{d}$.

Let $\delta = \sum_{c=1}^{r+1} (\lambda_c \cdot \beta_c + \overline{\lambda_c \cdot \beta_c})$. Using Hadamard's inequality, we bound $|S_c| \leq \left(\frac{p-3}{2}\right)^{\frac{p-3}{4}} = D_1$ and $|S| \leq \left(\frac{p-1}{2}\right)^{\frac{p-1}{4}} = D_0$. Then, using the fact that the choice of λ_c eliminates the first term in the expansion of f_c , we find that $|S| \cdot |\delta| \leq 2x^{(p-1)/2p} \cdot \sum_{c=1}^{r+1} |S_c| |R_{c,0}(x)|$, where $R_{c,0}(x) = f_c(x) - x^{(p-1)/2p}$. With the same arguments as in [Mi2], we deduce:

$$|S\delta| < 2(p-1)D_1 \cdot \frac{1}{|x|^{(p+1)/2p}}.$$

This inequality holds for all conjugates $\sigma_c(\delta)$, thus leading to:

$$|\mathbf{N}(S\delta)| < (2(p-1)D_1)^{(p-1)/2} \cdot \frac{1}{|x|^{\frac{(p-1)(p+1)}{4p}}}.$$

If $\delta \neq 0$, then $|\mathbf{N}(S\delta)| \geq 1$ and thus $|x| \leq 2^{5-p} \left(\frac{p}{2}\right)^{\frac{p}{2}}$. If $\delta = 0$, then $0 = S\delta = S \cdot |x|^{(p-1)/2} - \sum_{c=1}^{(p-1)/2} S_c R_{0,c}$, and thus:

$$|x| \leq \sum_c |S_c|/|S| < (p-1)D_1 < 3 \left(\frac{p-3}{2}\right)^{(p-3)/2}.$$

These bounds are better than the ones in [Mi2], and this concludes the clarification.

5.2. Proof of Lemma 2.7.

Proof. Let $\theta = \sigma_w \psi_u + \sigma_z \psi_v$. The conditions required by the lemma lead to the following linear system of equations over \mathbb{F}_n :

$$(20) \quad \begin{cases} w \cdot \varphi(\psi_u) & + & z \cdot \varphi(\psi_v) & = & 0 \\ 1/w \cdot \phi^{(-1)}(\psi_u) & + & 1/z \cdot \phi^{(-1)}(\psi_v) & \neq & 0 \end{cases}$$

Considered as a linear system in the unknowns $w, z \in \mathbb{F}_n$, the above system has the matrix $M = \begin{pmatrix} \varphi(\psi_u) & \varphi(\psi_v) \\ \phi^{(-1)}(\psi_v) & \phi^{(-1)}(\psi_u) \end{pmatrix}$. Assume that the product $P(t) = \varphi(\psi_t) \cdot \phi^{(-1)}(\psi_t)$ is not constant for all $t \in (\mathbb{Z}/n \cdot \mathbb{Z})^*$. Then there are two elements $u, v \in (\mathbb{Z}/n \cdot \mathbb{Z})^*$ such that $P(u) \neq P(v)$; for such values u, v , the matrix M is regular over \mathbb{F}_p and for any non vanishing right hand side in the second equation, the system has a unique solution (w, z) . For this choice of $u, v; w, z$, the element $\theta = \sigma_w \psi_u + \sigma_z \psi_v$ satisfies the condition of the lemma.

We now show that $P(t) : (\mathbb{Z}/n \cdot \mathbb{Z})^* \rightarrow \mathbb{F}_p$ is not a constant function. The proof uses explicit computations which include divisions by several constants which must be assumed to be non - null. Therefore we suppose that $n \notin E := \{3, 7\}$ and shall verify independently that the claim of the lemma holds for this exceptional set.

Let φ be the Fermat quotient map and Θ_k be the k -th Fuchsian. For any integer $1 < k < n - 1$, we have:

$$\begin{aligned} (n-k)^n - (n-k) &\equiv -k^n - n + k \pmod{n^2} \\ &\equiv -n \left(\frac{k^n - k}{n} + 1 \right) \pmod{n^2}. \end{aligned}$$

Dividing both terms by n and recalling from Lemma 2.6 that $\varphi(\Theta_k) = \varphi(k) \equiv \frac{k^n - k}{n} \pmod{n}$, we find:

$$(21) \quad \varphi(\Theta_{n-k}) = n - (1 + \varphi(\Theta_k)).$$

Using now (15) from Lemma 2.6, with $m = 2$, we find that:

$$\phi^{(-1)}(\Theta_k) \equiv \frac{k^3 - k}{2k^2} B_2 \equiv \frac{1}{12} \cdot \left(k - \frac{1}{k} \right) \pmod{n},$$

where we used the fact that $B_2 = 1/6$. Finally, using that $\psi_k = \Theta_{k+1} - \Theta_k$ for $k > 1$ while $\psi_1 = \Theta_2$, we obtain the following expressions for the moments of interest:

$$\begin{aligned} \varphi(\psi_k) &= \varphi(k+1) - \varphi(k), \\ \phi^{(-1)}(\psi_k) &\equiv \frac{1}{12} \cdot \left(1 + \frac{1}{k(k+1)} \right). \end{aligned}$$

Note that $\phi^{(-1)}(\psi_k) = 0$ iff $k^2 + k + 1 = 0$; if $n \equiv 1 \pmod{6}$, the equation has two solutions in \mathbb{F}_n , otherwise it has none. In the latter case $\phi^{(-1)}(\psi_k) \neq 0$ for all k .

We shall assume that P is the constant function and shall show that this assumption fully determines the Fermat quotient of integers in dependence of $\varphi(2)$, and this determination is in contradiction with (21); the contradiction implies that P cannot be constant, thus completing the proof.

Let thus $C = \varphi(2) \cdot \phi^{(-1)}(\Theta_2) = \varphi(2) \cdot \frac{1}{8}$. Assume first that $\varphi(2) = 0$ and recall from (21) that $\varphi(k) + \varphi(n-k) + 1 = 0$. Therefore at least $\frac{n-1}{2}$ of the values of φ are non-vanishing. Since $\phi^{(-1)}(k) \cdot (\varphi(k+1) - \varphi(k)) = 0$ for all k we see that if $n \not\equiv 1 \pmod{6}$, then φ is constantly vanishing, which is impossible.

If $n \equiv 1 \pmod{6}$, let $l, m \in \mathbb{F}_n$ be the non trivial third roots of unity, so $\phi^{(-1)}(\psi_l) = \phi^{(-1)}(\psi_m) = 0$, while for all $k \notin \{l, m\}$ we must have $\varphi(k+1) = \varphi(k)$. In particular, if $l < m$, there are two integers a, b such that

$$\varphi(2) = 0 = \dots = \varphi(l); \quad \varphi(l+1) = a = \dots = \varphi(m); \quad \varphi(m+1) = b = \dots = \varphi(n-1).$$

But $\varphi(n-1) = -1$ while $\varphi(n-2) = -1 - \varphi(2) = -1$, so $b = -1$. For symmetry reasons induced by (21), we must have $a = -1/2$ and $m = n - l$. This is absurd since $m^3 \equiv 1 \pmod{n}$ implies $l^3 = (n-m)^3 \equiv -m^3 \equiv -1 \pmod{n}$, so $n = 2 \not\equiv 1 \pmod{6}$. Thus $\varphi(2) \neq 0$ in this case too. Since $\phi^{(-1)}(l) = 0$, it follows however that $C = \varphi(l) \cdot \phi^{(-1)}(l) = 0$ and thus $C = 0 = \varphi(2)/8$ and we should have $\varphi(2) = 0$, in contradiction with the facts established above. Consequently, if $n \equiv 1 \pmod{6}$, then P cannot be constant.

We consider now the case $n \not\equiv 1 \pmod 6$, in which we know that $C \neq 0$. By expressing $C = P(2) = P(k)$ we obtain the following induction formula

$$\begin{aligned} C = \frac{1}{12} \cdot \frac{3\varphi(2)}{2} &= \frac{1}{12}(\varphi(k+1) - \varphi(k)) \cdot \frac{k^2 + k + 1}{k(k+1)}, \quad \text{hence} \\ \varphi(k+1) - \varphi(k) &= \frac{3\varphi(2)}{2} \cdot \frac{k(k+1)}{k^2 + k + 1}, \\ \varphi(3) - \varphi(2) &= \frac{9}{7}\varphi(2) \Rightarrow \varphi(3) = \frac{16}{7}\varphi(2). \end{aligned}$$

By eliminating $\varphi(2)$ from the above identity for two successive values of k one finds

$$\varphi(k+1) = \frac{2k^3}{k^3-1} \cdot \varphi(k) + \frac{k^3+1}{k^3-1} \cdot \varphi(k-1).$$

We shall use the reflexion formula (21) between the last and the first values in the sequence $1, 2, \dots, n-2, n-1$. Letting $k = n-2$ in the above induction, we find

$$\begin{aligned} -1 &\equiv \varphi(n-1) \equiv \frac{16}{9} \cdot \varphi(n-2) + \frac{7}{9} \cdot \varphi(n-3) \\ &\equiv \frac{16}{9} \cdot (-1 - \varphi(2)) + \frac{7}{9} \cdot (-1 - \varphi(3)) \pmod n, \\ 9 &\equiv 16 + 16\varphi(2) + 7 + 7\varphi(3) \equiv 23 + (16 + 7 \cdot \frac{16}{7})\varphi(2) \pmod n, \quad \text{hence} \\ -7 &\equiv 16 \cdot \varphi(2) \pmod n. \end{aligned}$$

Consequently $\varphi(2) \equiv -\frac{7}{16} \pmod n$ and thus $\varphi(3) \equiv \frac{16}{7}\varphi(2) \equiv -1 \pmod n$. But then (21) implies that $\varphi(n-3) = -1 - \varphi(3) = 0$, and thus $C = 0$, in contradiction with the previously obtained non vanishing fact. This confirms that $P(t)$ is non constant in this case too.

It remains to verify the claim for the exceptional primes in E . For $n = 3$ the Stickelberger ideal is trivial, so there is nothing to prove. For $n = 7$ one can repeat the proof of the case $n \equiv 1 \pmod 6$, which requires no division by 7; this completes the proof of the Lemma. \square

Acknowledgements: *The first author is grateful to the Universities of Bordeaux and Göttingen for providing a stimulating environment during the development of this work. Both authors thank Mike Bennett and Kalman Győry for suggesting this interesting problem for an algebraic investigation.*

REFERENCES

- [Be] M. A. Bennet: *Rational Approximation To Algebraic Numbers Of Small Height: The Diophantine Equation $|ax^n - by^n| = 1$* , J. Reine Angew. Math., **535**, pp. 1–49 (2001).
- [BGMP] M. A. Bennett, K. Győry, M. Mignotte and Á. Pintér: *Binomial Thue equations and polynomial powers*, Compositio Math. **142**, pp. 1103–1121 (2006).
- [BBM] Y. Bilu, Y. Bugeaud and M. Mignotte: *The problem of Catalan*, Springer (2014).
- [Bilu] Y. Bilu: *Catalan's conjecture (after Mihăilescu)*, Séminaire Bourbaki, Exposé 909, 55ème année (2002–2003); Astérisque 294, pp. 1–26 (2004).
- [BHM] Y. Bugeaud, G. Hanrot and M. Mignotte: *Sur l'équation diophantienne $\frac{x^n-1}{x-1} = y^q$* , III, Proc. London. Math. Soc. **84**, pp. 59–78 (2002).
- [BH] J. P. Buhler and D. Harvey: *Irregular primes to 163 million*, Math. Comp., **80:276**, pp. 2435–2444 (2011).
- [G] K. Győry: *Personal communication*.

- [Jha] V. Jha: *The Stickelberger Ideal in the Spirit of Kummer with Application to the First Case of Fermat's Last Theorem*, Queen's University, Queen's papers in pure and applied mathematics **93** (1993).
- [Mi1] P. Mihăilescu: *Primary cyclotomic units and a proof of Catalan's conjecture*, in *J. Reine Angew. Math.* **572**, pp. 167–195 (2004).
- [Mi2] P. Mihăilescu: *Class Number Conditions for the Diagonal Case of the Equation of Nagell and Ljunggren*, in *Diophantine Approximation*, Springer Verlag, Development in Mathematics **16**, pp. 245–273 (2008).